# Seguridad en *smartphones*

Los teléfonos celulares conocidos como *smartphones* (teléfonos inteligentes) son el sueño hecho realidad para muchos autores de ciencia ficción, pero quizá ni los mismos Arthur C. Clarke o Isaac Asimov habrían pensado que en solo unas cuantas décadas tendríamos en nuestras manos un dispositivo para uso personal que, además de realizar llamadas telefónicas, ayudara a organizar nuestra vida personal y laboral, lograra la comunicación por video, grabara voz e imágenes, sirviera como geolocalizador e incluso permitiera llevar a cabo transacciones comerciales y bancarias, todo ello con un solo dedo. En efecto, los *smartphones* están ocupando rápidamente el espacio que antes estaba reservado para computadoras, reproductores de música o cámaras digitales, para convertirse en auténticos equipos multifuncionales y asistentes personales, todo en uno.

Sin embargo, lo que aún no terminamos de asimilar es que la complejidad de estos aparatos los hace comportarse como cualquier otra computadora conectada a una red, con todos los riesgos que ello implica. De acuerdo con Gartner, empresa líder mundial en investigación y consultoría de tecnologías de la información, durante 2013 el sistema operativo para *smartphones* con más presencia fue Android, que abarcó el 78.4 % del mercado global, seguido de iOS con un 15.6 % y Microsoft con un 3.2 %. Por su parte, Forbes publica en su página web, también en 2013, que el 97 % de las amenazas (*malware*) estuvieron dirigidas hacia Android y menos del 1 % hacia IPhone iOS y Microsoft Windows Phone. Desafortunadamente, el crecimiento de amenazas dirigidas a dispositivos móviles va en aumento. En el documento 2014 Threats predictions, McAfee vaticina un incremento del 33 % del *malware* dirigido a este tipo de aparatos con respecto a las computadoras personales y que dicho aumento podría continuar durante todo 2014. Los datos anteriores son solo un ejemplo de los peligros potenciales a los que estamos expuestos si no tomamos las medidas adecuadas para evitarlos. Es fundamental comprender que los *smarthphones* podrían estar a merced de *hackers* o usuarios malintencionados que buscarán acceder a nuestra información para cometer fraudes o extorsiones. Nosotros mismos podríamos instalar, sin darnos cuenta, aplicaciones que contengan *malware* que provoquen bloqueos o busquen información que más adelante sea transferida hacia un equipo en particular; o quizá podríamos ser víctimas de ataques *man-in-the-middle* (intermediario), cuando el agresor accede a los mensajes, los modifica o añade sin que el emisor y el receptor se percaten de ello.

A pesar de lo anterior, las recomendaciones para evitar caer en manos de usuarios indeseables son relativamente sencillas:

Actualizar el sistema operativo. Los teléfonos inteligentes, como cualquier equipo de cómputo, deben actualizar su sistema operativo. Hacerlo permitirá corregir problemas que surjan durante su operación o eliminar vulnerabilidades de seguridad.

Asignar una contraseña. Es muy importante asignar una contraseña al equipo; afortunadamente algunos de ellos la solicitan por omisión. De esta manera, en caso de que el teléfono sea robado, será más difícil que la información contenida en él pueda ser utilizada.

Guardar el IMEI (International Mobile Equipment Identity). Este es un código que contienen los teléfonos celulares que los identifican y los hacen únicos a nivel mundial, es decir, no pueden existir dos teléfonos con el mismo IMEI. Para obtener este número, se puede acceder a los parámetros de configuración del teléfono o bien marcar *#06# sin presionar el botón "llamar" y automáticamente lo mostrará en pantalla. Es muy importante guardarlo en un lugar seguro, pues si nuestro *smartphone* es robado, es posible reportarlo con el proveedor del servicio proporcionando el IMEI para que de inmediato lo bloquee.

No usar la red Wi-Fi para ciertas operaciones. Procurar no hacer uso de las redes Wi-Fi públicas (llamadas *hotspots*) para realizar transacciones comerciales o bancarias. Generalmente estas redes son poco confiables y podría haber personas monitoreando su actividad, tratando de obtener la información que viaje a través de estas.

Emplear el *bluetooth* con cautela. Si no se está utilizando el *bluetooth* no lo active, y en caso de que lo haga, active la opción no visible. En un ambiente público habrá más de un usuario que pueda visualizar el teléfono e intentar acceder a él.

Instalar aplicaciones de fuentes confiables. Cada vez que se le pone un nuevo *software* al teléfono, es recomendable emplear fuentes confiables. Generalmente, sistemas operativos como iOS o Windows Phone no permiten hacerlo de fuentes distintas a las establecidas por los mismos proveedores; esto no significa que no puedan encontrarse aplicaciones falsas (*fake apps*) en ellos. Sin embargo, en el caso de Android, es factible realizar la instalación por distintas fuentes (SlideMe, GetJar o sitios web), lo que permite a los usuarios instalar una gran cantidad de aplicaciones para *smartphones* que no están debidamente auditadas, razón por la cual es relativamente sencillo agregar *malware* a dichas *apps*. Asimismo, será necesario constatar los recursos que la *app* utilizará, ya que existen aplicaciones gratuitas que solicitan tener acceso a las fotografías o a los contactos del dispositivo para poder verlos y utilizarlos.

Activar el GPS solo cuando se requiera. La gran ventaja de tener integrado un geolocalizador es que en caso de pérdida o robo, el teléfono

pueda ser ubicado; sin embargo, también encierra la desventaja de ser localizado por terceras personas cuyas intenciones sean hacer daño.

Instalar un antivirus. Así como crecen las ventas de los *smartphones*, también irán creciendo las amenazas asociadas con su *software*. Una forma saludable de disminuir la existencia del *malware* es mediante la instalación de un antivirus (McAfee, Kaspersky, Symantec, AVira o ESET).

Respaldar información. Es fundamental que la información contenida en un *smartphone* (contactos, notas, fotografías, videos, etc.) sea respaldada. Los teléfonos suelen tener sus propias aplicaciones para realizar esta tarea. Si el teléfono se extravía o es robado, al menos se contará con la información en un medio de respaldo alterno. Asimismo, es importante desactivar el autoguardado de fotografías, videos, archivos, etc., en la nube, en especial si son de índole personal.

Desechar el *smartphone* adecuadamente. Cuando se va a reemplazar el teléfono, ya sea porque finalizó su vida útil o porque se desea adquirir un modelo más reciente, es muy importante asegurarse de que la información contenida en él sea debidamente eliminada o destruida.

Sin duda alguna, los *smartphones* seguirán cautivando nuestra vida laboral y personal; sin embargo, es necesario tomar conciencia de las amenazas a los que están expuestos y aplicar las medidas necesarias para disminuir la presencia de *malware*, intrusos o robo de información.

Revisión técnica:
Ing. Julio Alfonso De León Razo
Ing. Mauricio Velázquez Álvarez

## REFERENCIAS

- Gartner, (2014). Gartner says annual smartphone sales surpassed sales of feature phones for the first time in 2013. Tomado de www.gartner.com/newsroom/id/2665715.
- Kelly, G (2014). Report: 97% of mobile malware is on android. This is the easy way you stay safe, *Forbes Magazine*. Tomado de www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/.
- McAfee Labs. (2013). McAfee Labs® 2014 Threats predictions. Tomado de www.mcafee.com/uk/resources/reports/rp-threats-predictions-2014.pdf.
- Smith, T. (2013). How do I protect the information on my smartphone?, vol. 8, ejemplar 2, NYS Office of Cyber Security Monthly Security Tips. Tomado de http://www.dhses.ny.gov/ocs/awareness-training-events/news/documents/2013-02.pdf.